UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,287	12/18/2001	John B. Hattick	IND10290	1861

22917 7590 05/31/2005

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,287	HATTICK ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 4, and 8 – 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Bush, "Secure Encryption of Data Packets for Transmission Over Unsecured Networks", U.S. Patent Publication, 2002/0002675 A1.

Regarding claim 1, Bush discloses:

an identification number associated with the data carrier (Bush, page 4, pars. 54, 55). Bush discloses a plurality of unique identification numbers that could be associated with the data carrier, such as an account number, bank number, and/or a personal identification number.

a memory for storing a one-time pad and data, wherein the one-time pad is uniquely associated with the identification number (Bush, page 2, par. 25; page. 3, par. 35, lines 4,5).

an encryption circuit, coupled to the memory, for encrypting the data with

the one-time pad (Bush, page 3, par. 35, lines 4,5; page. 5, par. 56, lines 16,17).

and a controller, coupled to the memory, to prevent reuse of bits in the one-time pad (Bush, page 3, par. 33; page 5, par. 65).

Regarding claim 2, Bush discloses:

wherein the encryption circuit performs an exclusive-or function (Bush, page 3, par. 40).

Regarding claim 3, Bush discloses:

the data carrier of claim 1 further comprising a counter, coupled to the memory, to index to a next bit in the one-time pad (Bush, page 3, par. 32, par. 40). The system of Bush comprises the encoding/decoding of digital data. Bush discloses that the counter indexes to the next available position in the one time pad, whereupon a XORing of the bits of the one time pad and the data will occur. Thus, Bush discloses indexing to a next bit in the one time pad.

Regarding claim 4, Bush discloses:

the data carrier of claim 1 further comprising an interface, wherein the interface comprises at least one of the following: capacitive coupling, inductive coupling, electromagnetic coupling, optical coupling, electrical coupling, and contact (Bush, page 5, par. 56). Bush discloses the data carrier embodied as a PCMCIA device and a contact interface with a receiving device.

Regarding claim 7, Bush discloses:

the data carrier of claim 1 wherein the one-time pad is generated by one of the following: a true random number generator, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier (Bush, page 1, par. 7; page 2, par. 30).

Regarding claim 8, Bush discloses:

the data carrier of claim 1 for use with a reader, wherein the reader comprises a generator to generate the one-time pad via one of the following: a look-up table, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier (Bush, fig. 6, elems. 602, 604; page. 5, par. 59). Bush discloses the carrier-receiver interface being directly attached to processor 604, thus a device comprising a generator which generates the one time pad via a look-up table ("list").

Regarding claim 9, Bush discloses:

a memory storing data and a one-time pad (Bush, page 2, par. 25; page. 3, par. 35, lines 4,5).

an index to synchronize a starting position in the one-time pad (Bush, page 3, par. 32).

an identification number uniquely associated with the one-time pad (Bush, page 4, pars. 54, 55).

and a transmitter to transmit the data to the reader (Bush, fig. 6, elems. 614, 602).

Regarding claim 10, Bush discloses:

a generator to generate the one-time pad (Bush, fig. 6, elems. 602, 604; page. 5, par. 59).

and a receiver to receive data from the data carrier (Bush, fig. 6, elems. 602, 604).

Regarding claim 11, Bush discloses:

the data carrier of claim 10 wherein the receiver further receives the index from the data carrier to synchronize with the starting position in the one-time pad (Bush, page 3, par. 32; page 4, pars. 45, 53; fig. 4). Bush discloses the one time pad as being divided into fixed length blocks of bits, or "sheets". The carrier encodes a block of data with its corresponding sheet from the one time pad, and sends the encoded sheet to the receiver. That is the signal for the reader to update its index pointing to the next sheet from the one time pad. Thus the receiver receives the index from the data carrier.

Regarding claim 12, Bush discloses:

the data carrier of claim 10 wherein the data carrier and the reader communicate via one of the following interfaces: capacitive interface, inductive interface, electromagnetic interface, optical interface, electrical interface and

contact interface (Bush, page 5, par. 56). Bush discloses the data carrier embodied as a PCMCIA device and a contact interface with a receiving device.

Regarding claim 13, Bush discloses:

the data carrier of claim 10 wherein the generator generates the one-time pad by one of the following: a look-up table, and a pseudorandom number generator operating on a secret key and the identification number of the data carrier (Bush, fig. 6, elems. 602, 604; page. 5, par. 59). Bush discloses the carrier-receiver interface being directly attached to processor 604, thus a device comprising a generator which generates the one time pad via a look-up table ("list").

Regarding claim 14, Bush discloses:

the data carrier of claim 9 further comprising a controller to prevent reuse of bits in the one-time pad (Bush, page 3, par. 33; page 5, par. 65).

Regarding claim 15, Bush discloses:

the data carrier of claim 9 further comprising a counter to index to a next bit in the one-time pad once a bit has been used (Bush, page 3, par. 32, par. 40). Bush discloses a counter to index to the beginning of the next sheet, thus a next bit usable for encryption, once a previous sheet has been disposed of, marking the advent of a last bit used for encryption.

Regarding claim 16, Bush discloses:

the data carrier of claim 9 wherein the data is stored in a first memory and the one-time pad is stored in a second memory (Bush, fig. 1; page 2, par. 25; page 3, par. 35). Bush discloses the storing of individual blocks of bits, "sheets" of the one time pad in ROM. Also disclosed is the storing in a second location, physically securing separately, of software or "data" on the device.

Claim 21 is rejected under 35 U.S.C. 102(b) as being anticipated by Menezes et al., Handbook of Applied Cryptography.

Regarding claim 21, Menezes et al. discloses:

providing an identification number (Menezes et al., page 193, fig. 6.1). Menezes et al. discloses providing to the cipher generator an number identifying the initial state of the machine ("identification number").

providing a secret key (Menezes et al., page 193, fig. 6.1). Menezes et al. discloses providing a secret key (k).

encrypting the identification number with the secret key (Menezes et al., page 193, fig. 6.1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush in view of La Porte, "PCMCIA Card and Card Socket Power Management".

Regarding claim 5, Bush discloses that his data carrier is embodied as a PCMCIA device. He does not disclose the data carrier of claim 1 further comprising a power supply that receives energy from a reader via at least one of capacitive coupling, inductive coupling, electromagnetic coupling, optical coupling, and contact.

La Porte, discloses a description of the PCMCIA device specification. La Porte shows that PCMCIA cards draw power from their host system via capacitive coupling ('reader') (La Porte, page 1, fig. 1; page 2, par. 3).

It would have been obvious to one of ordinary skill in the art to employ the power supply design of PCMCIA cards for receiving external energy by La Porte with the PCMCIA card of Bush. This would have been obvious because one of ordinary skill in the art would have recognized this to be the specified and typical design and operation of PCMCIA cards.

Regarding claim 6, the combination of Bush and La Porte discloses: *The data carrier of claim 1 further comprising a power supply that receives energy from one of the following: a battery, and a super-capacitor* (La Porte, page 1, fig. 1; page 2, par. 3).

Claims 17 – 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush in view of Menezes et al., Handbook of Applied Cryptography.

Regarding claim 17, Bush discloses *storing a set of data and a one-time pad, wherein the one-time pad is uniquely associated with an identification number* (Bush, page 2, par. 25; page. 3, par. 35, lines 4,5), and *synchronizing the one-time pad and an index value with an external device to establish a starting position in the one time pad* (Bush, page 3, par. 32; page 4, par. 45; fig. 4). Bush also discloses the receiving of a random skip value from the external device (Bush, page 4, par. 53; page 5, par. 61). As disclosed an external device can provide the carrier with an checkbook as well as instructions for randomly varying the starting position of the one time pad.

Bush does not disclose utilizing the one time pad in requesting and receiving from the external device a number of bits, and if the requested and received bits match, then continuing to employ the one time pad according to the conditions imposed from the consumption of the bits of the one time pad during the challenge-response and the random starting position designated by the external device.

Menezes et al. discloses a method for authenticating messages from a sender and receiver and for preventing relay attacks. This challenge-response method comprises a first entity sending a random number to a second entity, and subsequently receiving the random number repeated by the second entity to the first. Menezes et al. discloses the repeated message or random number should be cryptographically bound or encrypted with a symmetric key so as to prevent misuse by adversaries. If the second entity correctly responds to the challenge, then the communication shared between the two entities is deemed 'fresh' or authentic (Menezes et al., pages 397-402, section 10.3; page 398, "Random numbers", pars. 1-3; page 401).

It would have been obvious to one of ordinary skill in the art to employ the encrypted challenge-response method of Menezes et al. with the one time pad communications system of Bush involving a data carrier and external device. This would have been obvious because one of ordinary skill in the art would have been motivated to provide measures of security, and a secured authentication of the external device to the carrier would provide such measures of security. Thus the combination of Bush and Menezes et al. discloses the sending a challenge encrypted by the key held by the carrier ("requesting a number of bits"), receiving the challenge encrypted with the key held by the external device ("receiving a set of bits"), and comparing the challenge with response to determine authenticity. Since the combination of Bush and Menezes et al. teaches the encryption of the challenge and response, the combination also discloses the consumption of bits from the one time pad, and thus the need to increment the index.

Regarding claim 18, the combination of Bush and Menezes et al. discloses:

generating the one-time pad based on the identification number (Bush, fig. 6, elems. 602, 604; page. 5, par. 59). Bush discloses the carrier-receiver interface being directly attached to processor 604, thus a device comprising a generator which generates the one time pad via a look-up table ("list"), producing the pad by identifying the check associated with it.

and receiving the index value to synchronize with the starting position in the one-time pad (Bush, page 3, par. 32; page 4, pars. 45, 53; fig. 4). Bush discloses the one time pad as being divided into fixed length blocks of bits, or "sheets". The carrier encodes a block of data with its corresponding sheet from the one time pad, and sends the encoded sheet to the receiver. That is the signal for the reader to update its index pointing to the next sheet from the one time pad. Thus the receiver receives the index from the data carrier.

Regarding claim 19, the combination of Bush and Menezes et al. discloses:

the method of claim 18 wherein the step of generating comprises encrypting the identification number with a secret key (Bush, page 4, par. 54). As disclosed by Bush, the electronic checkbook, is a collection of encoded data packets including the encryption of the identification number.

Regarding claim 20, the combination of Bush and Menezes et al. discloses:

associating an identification number with a one time pad (Bush, page 2, par. 25; page. 3, par. 35, lines 4,5).

storing the identification number, one-time pad and data on the data carrier (Bush, page 2, par. 25; page. 3, par. 35, lines 4,5).

setting an index, wherein the index identifies a next available bit of the one-time pad (Bush, page 3, par. 32, par. 40). The system of Bush comprises the encoding/decoding of digital data. Bush discloses that the counter indexes to the next available position in the one time pad, whereupon a XORing of the bits of the one time pad and the data will occur. Thus, Bush discloses indexing to a next bit in the one time pad.

transmitting the identification number, the index and a challenge to the reader, wherein the challenge at least requests transmission of bits of the one-time pad (Bush, page 4, par. 54; fig. 6, elems. 614, 602, 612, 604; also see explanation regarding claim 17) *;*

generating the one-time pad in the reader based on the identification number (Bush, fig. 6, elems. 602, 604; page. 5, par. 59). Bush discloses the carrier-receiver interface being directly attached to processor 604, thus a device comprising a generator which generates the one time pad via a look-up table ("list"), producing the pad by identifying the check associated with it.

transmitting bits of one-time pad, based on the index and challenge and a random skip value, from the reader to the data carrier and verifying, at the data carrier, that the bits transmitted from the reader correspond to the challenge, and if correct,

incrementing the index by number of bits in the challenge and the skip value, and encrypting and transmitting at least a portion of the data to the reader (see explanation regarding claim 17).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Schneider et al., "Efficient Commerce Protocols Based on One-Time Pads.", Princeton University, IEEE 12/2000.

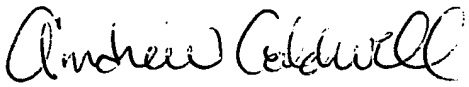
A shortened statutory period for reply is set to expire 3 months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Jeffery Williams
571.272.7965
5.19.2005